INFORMATION ASSURANCE AND SECURITY INTEGRATIVE PROJECT

SMART GRID PRIMER

JEFF ROTENBERGER

TS5910 Information Assurance and Security Integrative Project

Dr. Randy Stauber

March 15, 2012

Abstract

This project paper describes smart grid implementation, its advantages, and potential risks and concerns to consumers. It gives an overview of the state of the electrical grid and the electrical profile of the state of North Dakota. It then covers what smart grid is, some of the technologies involved and why it might be implemented. The paper also discusses some of the potential security and privacy risks related to consumer electrical usage data and mitigation strategies. It also covers current privacy laws and protections as well as their strengths and weaknesses. Finally, the role of state government and its agencies in protecting its constituents is discussed.

Table of Contents

Abstract....2
Introduction....7
State Electrical Profile....7
What is Smart Grid?....13
Current Smart Grid Technologies....14
Business Impacts....17
Why Smart Grid?....17
Reliability:....17
Efficiency....18
Security....18
Enhanced Customer Service....18
Risk Assessment....19
Information Security....21
Physical Security....27
Access Controls....29
Communication, Transmission and Network security....30
Incident Response....33
Preparation....34
Detection and Analysis....34
Incident Classification....35
Response....35
Follow up....36
Reporting....37
Disaster Recovery and Business Continuity....37
Business Continuity Plan....38
Ethical and Legal Implications....39
What's in the Data?....39
What are the risks?....41
Data Protections....45
The State's Role....47
Emergency Planning and Management....47
Citizen Advocation....48

Conclusion 48
GLOSSARY 49
Term 49
Definition 49
References 53
APPENDIX A HOME ENERGY CONTROLLER EXAMPLE 58
APPENDIX B PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS) 59
APPENDIX C INCIDENT HANDLING RESOURCE LIST 60
APPENDIX D SANS INCIDENT LOG SHEET 61
APPENDIX E EXAMPLE MEMORANDUM OF AGREEMENT 62

List of Tables

Table 1 - North Dakota Electric Generation by Source 8

Table 2 - North Dakota's 10 Largest Power Plants by Capacity 10

Table 3 - North Dakota's Top Five Retailers of Electric Energy (Values in MWh) 10

Table 4 - Data Classification Definitions and Examples 25

Table 5 - Risk Level Definitions 26

Table 6 - Example Technical Controls 29

Table 7 – Incident Classification 35

Table 8 - Privacy Concerns from Smart Grid 41

List of Figures

Figure 1 - Electric Energy Production by Source Figure 2 - Electric Energy Capacity by Source..... 9

Figure 3 Electric Energy Exports..... 11

Figure 4 - North Dakota Major Electric Interconnections..... 12

Figure 5 - North Dakota Map of Rural Electric Cooperatives..... 13

Figure 6 - Smart Grid Example..... 14

Figure 7 - Daily Electrical Load Curve Example..... 16

Figure 8 - Threat Matrix..... 19

Figure 9 - Smart Grid Communications..... 22

Figure 10 - The CIA Triangle..... 23

Figure 11 - Example Security Zone Requirements..... 29

Figure 12 - Cryptography Diagram..... 31

Figure 13 - Symmetric Cryptography..... 32

Figure 14 - Assymetric Cryptography..... 32

Figure 15 - Incident Response Lifecycle..... 34

Figure 16 - Wireshark Screenshot..... 36

Figure 17 - Example Daily Home Electrical Use..... 40

Introduction

Our lives revolve around electricity. As you sit and read this, think about how many electronic devices were needed to deliver it to your eyes; a computer, mouse, keyboard, lights, and possibly a printer. Or think back how to your morning routine was impacted by electricity; hot water for your shower, food from the refrigerator, coffee from the coffee maker, toast from the toaster, etc. It is typically something we take for granted. We use it, we get a bill every month and we pay for it.

What many people do not know is that over 40% of the energy used in the United States goes to creating electricity (Energy Information Administration, 2009). It comes to you every day across what is called the 'grid'; an interconnection of power generation and wires that bring electricity to your work and home. Unfortunately, today's grid struggles to keep up with the demand and cannot handle expected future consumption.

A more robust, 'Smart Grid' is imperative, employing new technologies to more effectively deliver electricity reliably where and when it is needed. While North Dakota currently does not have any major implementations of smart grid technologies, it is only a matter of time before it takes place. It is important then to understand the profile of electrical distribution within the state, what smart grid is (and is not) and what some of the benefits and concerns are.

State Electrical Profile

Electricity generation and demand are both low in North Dakota, commensurate with the State's population (Energy Information Administration, 2012). North Dakota exports a significant portion of its total electrical energy production to neighboring states and a small amount internationally. Coal-fired plants provide nearly all of North Dakota's electricity generation. Several large surface mines in the central part of the State supply most of the coal used for power generation. State coal production is substantial, and North Dakota brings in only small amounts of coal from other States. Hydroelectric dams and wind energy account for most of the State's non-coal electricity. The Garrison Dam, located about 75 miles northwest of Bismarck, is North Dakota's fifth largest plant in electricity generation capability.

North Dakota is a substantial producer of wind energy, with over 20 operational wind power projects, and leads the Nation in potential for wind power. Nearly three-tenths of North Dakota households use electricity as their primary energy source for home heating (Energy Information Administration, 2012).

Table 1 - North Dakota Electric Generation by Source

Net Electricity Generation	North Dakota	Share of ND	Share of U.S	As of date
Total Net Electricity Generation	2,789 gWh	100%	0.8%	Dec-2010
Petroleum-Fired	3 gWh	0.1%	0.2%	Dec-2010
Natural Gas-Fired	NM	NA	NA	Dec-2010
Coal-Fired	2,110 gWh	74.8%	1.5%	Dec-2010
Nuclear	-	-	-	Dec-2010
Hydroelectric	258 gWh	3.8%	0.8%	Dec-2010
Other Renewable	411 gWh	5.0%	2.5%	Dec-2010

The majority of North Dakota's electric energy production (nearly 75%) is coal-based and renewable energy is growing, currently producing nearly 8.8%. In March 2007, North Dakota adopted a voluntary renewable portfolio objective that aims to have one-tenth of electricity generated from renewable sources by 2015.

Renewable energy sources can be considered for utilization to provide energy supply when conventional sources are not 100% available, for example during a coal plant outage due to any number of factors. However, it is important to recognize the significant difference between capacity and production, as illustrated in Figures 2 and 3 below. For example, while wind energy comprises 14.5% of North Dakota's electric capacity, it only contributes 5.17% to energy production due to variations in wind patterns.

Figure 1 - Electric Energy Production by Source

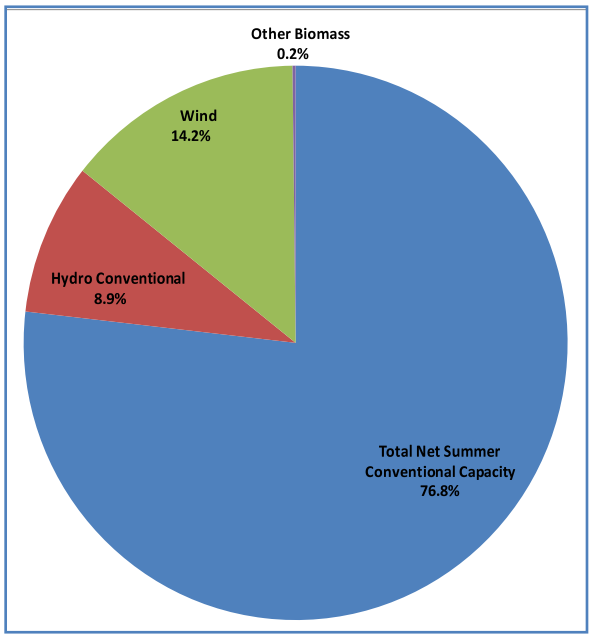
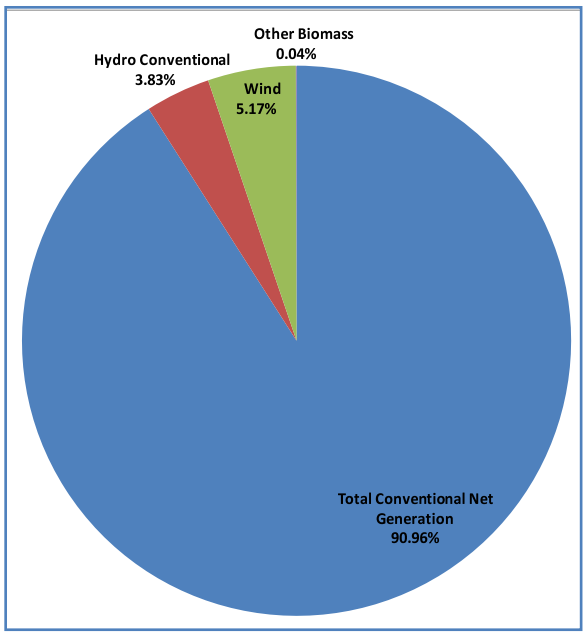


Figure 2 - Electric Energy Capacity by Source



North Dakota has considerable fossil fuel reserves. Coal is extracted from large surface mines in central North Dakota. Substantial crude oil and natural gas reserves are located in the Williston Basin, in the western part of the State. Although a low population largely accounts for the State's low total energy consumption, North Dakota's per capita energy consumption ranks among the highest in the Nation, in large part due to high demand for heating during the cold winters and an energy-intensive economy. Industry accounts for nearly one-half of the State's total energy consumption (Energy Information Administration, 2012). Table 2 below lists the major power plants in North Dakota and further illustrates the state's dependence on coal.

Table 2 - North Dakota's 10 Largest Power Plants by Capacity

Plant	Primary Energy Source or Technology	Operating Company	Net Summer Capacity (MW)
1. Coal Creek	Coal	Great River Energy	1,116
2. Antelope Valley	Coal	Basin Electric Power Coop	900
3. Milton R Young	Coal	Minnkota Power Coop, Inc	697
4. Leland Olds	Coal	Basin Electric Power Coop	669
5. Garrison	Hydroelectric	USCE-Missouri River District	486
6. Coyote	Coal	Otter Tail Power Co	427
7. Stanton	Coal	Great River Energy	188
8. Tatanka Wind Power LLC	Other Renewables	Acciona Wind Energy USA LLC	180
9. Langdon Wind LLC	Other Renewables	FPL Energy Langdon Wind LLC	159
10. FPL Energy Ashtabula Wind LLC	Other Renewables	FPL Energy Ashtabula Wind LLC	149
MW = Megawatt.			
Source: U.S. Energy Information Administration, Form EIA-860, "Annual Electric Generator Report." - 2008			

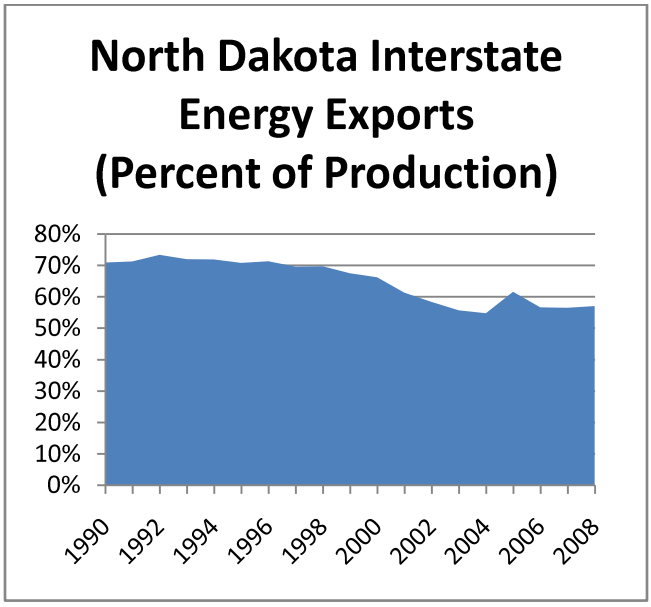
Three investor-owned electric utilities and two major cooperatives distribute over half of the state's energy production as shown in Table 3 below.

Table 3 - North Dakota's Top Five Retailers of Electric Energy (Values in MWh)

Entity	Type of Provider	All Sectors	Residential	Commercial	Industrial
1. Northern States Power Co - Minnesota	Investor-Owned	2,210,146	761,934	1,120,009	328,203
2. Otter Tail Power Co	Investor-Owned	1,619,082	572,647	964,373	82,062
3. Montana-Dakota Utilities Co	Investor-Owned	1,552,167	584,225	805,790	162,152
4. Basin Electric Power Coop	Cooperative	1,003,970	n/a	n/a	1,003,970
5. Cass County Electric Coop Inc	Cooperative	936,578	516,254	352,652	67,672
Total Sales, Top Five Providers		7,321,943	2,435,060	3,242,824	1,644,059
Percent of Total State Sales		59	57	73	44
Source: U.S. Energy Information Administration, Form EIA-861, "Annual Electric Power Industry Report." - 2008					

Even though North Dakota's per capita energy consumption ranks among the highest in the Nation, a significant portion of its electricity generation is exported, in the range of 50% to 60% as depicted in Figure 3 below.

Figure 3 Electric Energy Exports

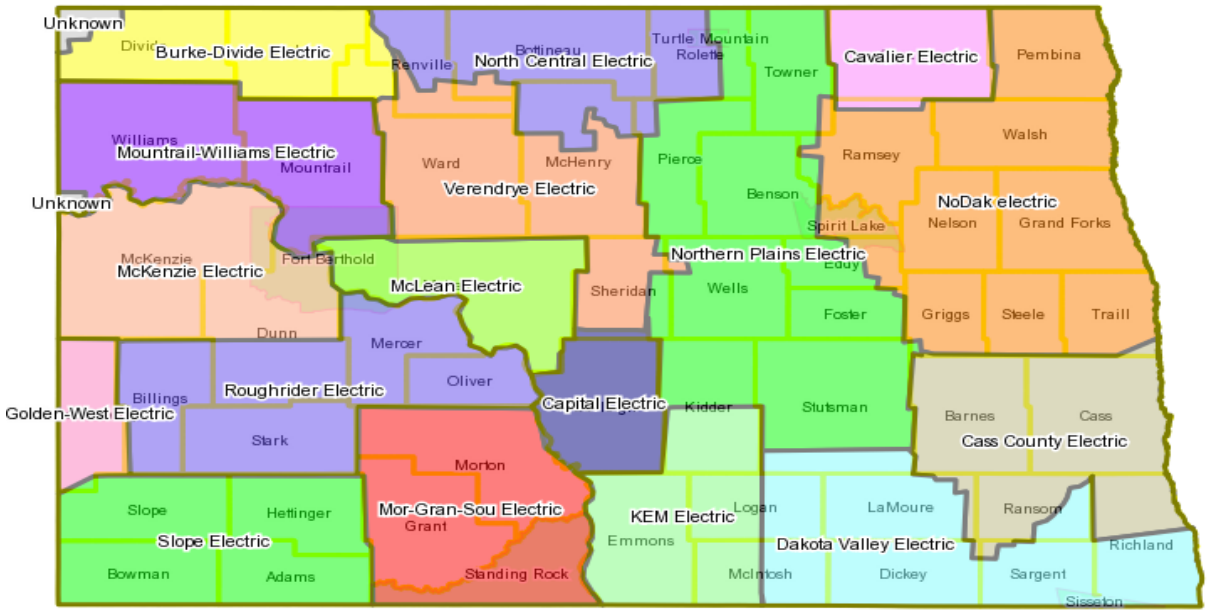


This underscores the importance of the electric transmission system and its availability to continuously move energy to markets. A breakdown in the interstate export electric transmission system that does not produce a system collapse could force major power plants to severely curtail output or be shut down. Given that the majority of electric generating plants are coal-fired, such a forced shut down could damage equipment and require lengthy restart periods. North Dakota's backbone transmission system is predominately 230 kV (kilovolts), but 138 kV provides remote area transmission service. There are presently two 345 kV lines primarily serving as interconnections into South Dakota.

Figure 4 - North Dakota Major Electric Interconnections

And additional challenge in North Dakota is that the state has a large number of rural electrical coops and three investor owned utilities that make up the entire state. A map of the coverage by utility is show in Figure 5 below.

Figure 5 - North Dakota Map of Rural Electric Cooperatives



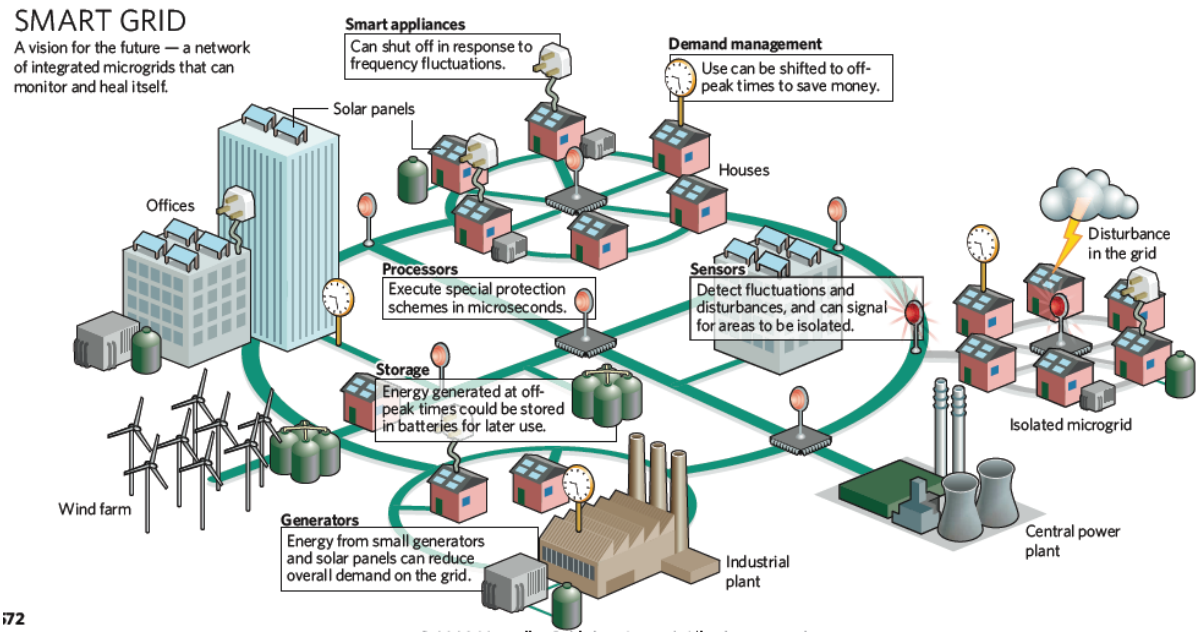
What is Smart Grid?

In North Dakota as well as throughout the rest of the United States, the electrical grid has developed over the last one hundred plus years as a scattered mix of local and regional power plants interconnected only to provide backup power in case of failure. When these regions needed more power, they simply built a new power plant and spliced it into the grid. Since the 1970s, however, changes to government regulations on how utilities operate have forced more power through lines that are barely able to handle it. In essence, the grid is inefficient. A good example is the 2003 blackout in northeastern US and eastern Canada, the result of which caused a $6 billion loss in revenue (U.S. Department of Energy, 2008). A simple transformer failure left many without electricity for over a week. Similar examples often happen in North Dakota due to acts of nature: winter and summer storms, flooding, etc. Depending on the length and severity of the storm or flood, consumers within the state can go without electricity for several days to even weeks before power is restored.

Because of this, modernization efforts to make the grid “smarter” are taking place throughout North America. “Already, some 8 million "Smart Meters," with the ability to conduct two-way

communication with utility companies, have been installed in U.S. homes. There will be nearly 50 million by 2012 (Sullivan, 2009)". The grand vision: upgrade power meters and electronic devices so they all constantly communicate with the result of "lower power consumption, lower power bills, people and planet happier" (Sullivan, 2009). An example of what the Smart Grid would look like is shown in Figure 6 below.

Figure 6 - Smart Grid Example



(Amin, 2008)

A grid system such as detailed above would allow for more resiliency, better efficiency and would detail customer usage down to the appliance level. It would allow for two-way flow of electricity *and* information within the transmission grid. While implementation of such technology within North Dakota is limited at present, it is important as it become more prevalent to understand what it is, what it does and how it can impact each of us.

Current Smart Grid Technologies

Many of the technologies and concepts involved in a smart grid implementation are not new. However, when combined together with digital communication its potential begins to be realized (U.S. Department of Energy, 2008). It can improve power reliability and quality and has safety, efficiency,

environmental and financial benefits. It also allows for greater integration of renewable energy sources such as wind and solar power.

At the consumer level and most visible of smart grid technologies is Advanced Metering Infrastructure (AMI). AMI is a method of enabling consumers to be more efficient in their electrical use while providing utilities the ability to monitor their grid. These types of devices could be deployed individually but most likely would be implemented as part of a Home Area Network (HAN) similar to a home wireless network but using a different band frequency and designed specifically for home electrical devices. This combination would allow for devices to be powered according the consumer's wishes, taking into account the near real-time pricing of electricity. In other words, your appliance could be programmed to run when it costs you the least to do so (U.S. Department of Energy, 2008). An example of a controller for such a system is shown in Appendix A. Energy usage could also be managed via a web application or even a smart phone.

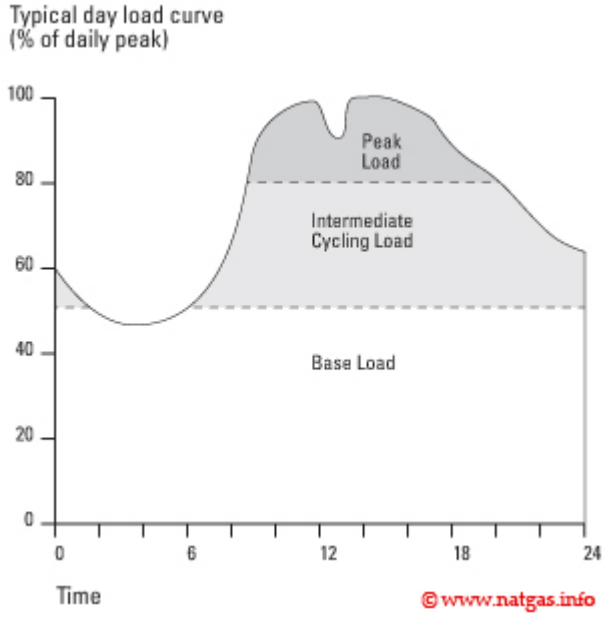
Grid management involves modernizing a large and very complex electrical distribution system that consists of thousands of transformers affecting millions of customers (National Organization of State Energy Officials, 2011). By modernizing and updating control systems along with integrating smart grid technologies, distribution systems will be optimized, automated and capable of self-healing.

Outage/management and recovery: These technologies have the ability to dramatically improve outage detection by providing a near instant notification which is not currently available to most distribution operators. By knowing when and where outages occurred, causes can be more quickly and easily determined (National Organization of State Energy Officials, 2011).

Voltage optimization/reduction/conservation: By optimizing the voltage in a distribution line, losses can be reduced within the line and some appliances without affecting performance. Phasor Measurement Units (PMU) are sensors that sample the voltage and current at a location many times per second. This sampling allows for dynamic real-time observation of the state of the grid, which in turn will facilitate response, reliability and efficiency.

One on the largest issues the electrical industry has to contend with is how to handle demand 'peaks', mostly because of the need to consume electricity as soon as it is generated. Not being able to predict when peaks may occur, generation must factor in a buffer to mitigate any potential spikes in demand. This problem becomes more pronounced during extreme usage, hot summer days, for example.

Figure 7 - Daily Electrical Load Curve Example



(Chandra, 2009)

The figure above shows an example of the changes in electrical demand in a typical day. Large generation plants that have high fixed cost but are cheap to operate and do so nearly continuously typically handle peak load. Plants that have lower fixed costs but very high operating costs handle intermediate and peak load generation. As a result, operating appliances during these times is more expensive as that cost is passed on to consumers. There are two ways that smart grid can impact this 'peak': enabling customers to control usage during the peak and enabling utilities to shed load without inconveniencing the customer. Examples of devices that could be cycled in this manner include water heaters, Heating, Ventilation, and Air Conditioning (HVAC), Plug-in Hybrid Electric Vehicle (PHEV)(chargers and batter components), distributed generation and storage, solar batteries, dryers, pool pumps and lighting. (U.S. Department of Energy, 2011).

This type of demand response would reduce the cost of handling electrical peaks and could potentially limit the need to use or create peak generation plants.

Smart grid technologies are more than just new meters. It is a combination of a number of applications and technologies that allow for a more intelligent use of generated electricity.

Business Impacts

Why Smart Grid?

There are a wide range of reasons a 'smart grid' makes sense, but the largest is simply that electrical demand has continued to grow while the infrastructure to handle that growth has not. Since 2000, only 668 miles of interstate electrical transmission have been built. Yet since 1982, peak demand for electricity has exceeded transmission growth by nearly 25% each year. This creates a system that is overtaxed during peak demands, leading to outages and power quality issues that cost U.S. businesses on average $100 billion per year (U.S. Department of Energy, 2008).

Additionally, our country has changed and North Dakota is a perfect example of that change. Renewable energy sources and environmental impacts are more prevalent in consumer's minds and it is evident here in our state with the wide range of energy sources that include wind, coal, oil, hydroelectric, etc. The grid needs to be able to integrate these technologies and leverage their advantages to improve the efficiency and efficacy of electrical distribution. Other reasons a smart grid makes sense:

Reliability: The number of black and brownouts has increased in this country, often due to the slow response time of dated mechanical switches, poor line of sight to the real-time grid situation and a lack of automated control analytics (U.S. Department of Energy, 2008). The adverse effects from these outages is more than just the lights not coming on; industry can be halted, food can spoil, financial transactions are impacted, and traffic lights are dark. The winter storm that hit the northwestern part of North Dakota in April of 2011 halted oil production within the region for several days, impacted the availability of flowers for Mother's Day, and cost one local grocery store up to $300,000 in lost inventory

due to food spoilage (Donovan, 2011). A smart grid will bring quicker response to outages; allow for integration of renewable energy sources, and increase the resiliency of the grid.

Efficiency: Because electricity has to be used essentially as soon as it is generated, the grid needs to be efficient; unfortunately it is not. Because of the complexity that has arisen from integrating a hotchpotch of regional and local grids into a larger nation-wide grid, the shutdown of even one transmission line can have cascading effects across large swaths of area. High demand due to time of day or extreme heat or cold can have the same effect. An improved grid can bring a near real-time picture of the grid status, match generation capacity to predicted demand and 'self-heal' by shutting down portions of the grid if fluctuations are detected and restore them afterwards (Amin, 2008). In some cases demand can be managed at the consumer level as well allowing utilities to shed load if needed. Other efficiencies may not be as evident: reduced overhead and manpower costs. For example, Advanced Metering Interfaces would eliminate the need to someone to manually read the meter. Likewise, knowing exactly where a break has occurred in a transmission line means less time searching for the downed line.

Security: Unless the cause of a blackout is immediately known (weather for instance), the experience can make citizens fear the worst. Five major blackouts have occurred in the last 40 years and three of those in the past nine years. The 2003 blackout, the worst in US history, caused many to believe the country was again the target of terrorism. Because of the electrical grid's current structure, it is open to attack. Interdependencies can easily cause cascading effects that would have a negative impact on financial institutions, communication, and security systems. A smarter grid would have cyber security features build into everything from systems to physical plant monitor and access control (National Organization of State Energy Officials, 2011).

Enhanced Customer Service: For most North Dakota electrical customers, management of electrical consumption happens as a reaction to their monthly bill or an outage. Smart grid technology would allow consumers to see their electrical usage on a daily or even hourly basis. Appliances within the household could be connected to a Home Area Network, which would allow homeowners to monitor usage on an individual appliance basis and program usage when electrical prices are lowest. Utilities

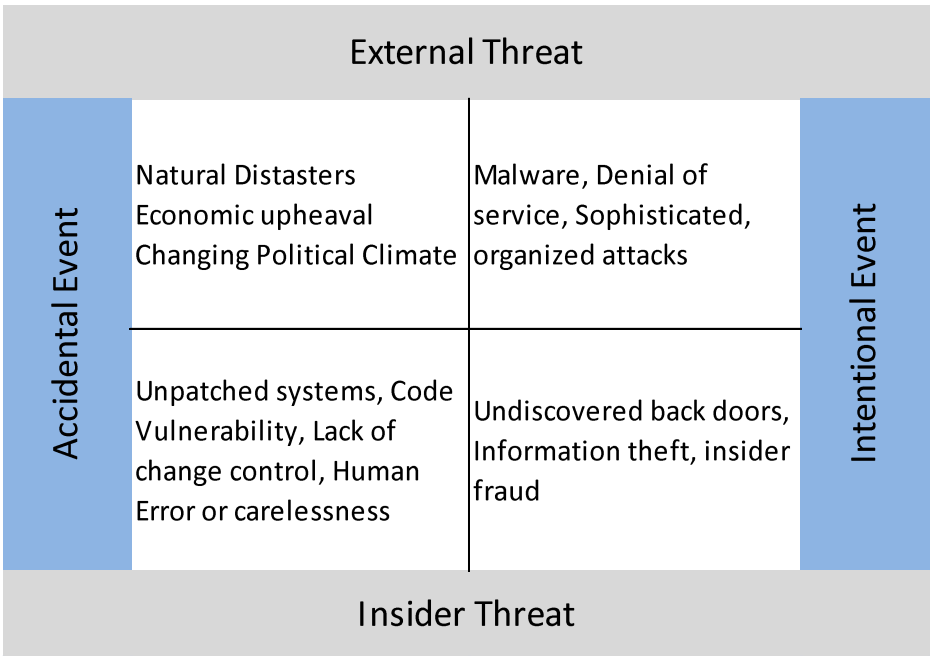
could access the network to shed load at peak demand and provide more detailed billing, potentially suggesting to customers ways to reduce their electrical bill (Siddiqui, 2008).

Risk Assessment

As utilities evaluate the implications of a smart grid implementation, they must decide how it will impact their business as well as where and how much of this data will be stored and for how long. They must also consider how such data will be collected, transmitted and stored securely. Consumers should be aware of what data is being gathered regarding electrical use and how utilities intend to use that data. State agencies must understand the potential data security and privacy risks and ensure that laws and regulations properly protect consumers.

A review of threats for Smart Grid technology results in the following matrix:

Figure 8 - Threat Matrix



(Danahy, 2009)

The most common threats in North Dakota are those that occur on the left side of the matrix. Natural disasters, specifically severe weather happen almost every year and often cause widespread electrical outages. North Dakota is subject to a number of weather-related emergencies, particularly

flooding. Over the 1964-2010 period, there were 32 instances of flooding, caused by major storms, excessive rainfall or snow/ice melts. Threats on the right side of the matrix are not new but are becoming more and more prevalent for a whole host of reasons: increased connectivity, system complexity and the fact that devices now do more than they ever were intended to do. Only recently has significant focus been put toward developing standards to address these types of threats. Some real examples of these:

- April/May 2007: the Estonian economy was largely shut down by cyber attacks originating in Russia over a statue of Stalin
- 2009 cyber attacks of Georgia prompted NATO comments.
- In 2001, hackers penetrated the California Independent System Operator; attacks were routed through California, Oklahoma, and China.
- Ohio Davis-Besse nuclear power plant safety monitoring system was offline for 5 hours due to Slammer worm in January 2003.
- Aaron Caffrey, 19, brought down the Port of Houston in October, 2003. This is thought to be the first well-documented attack on critical U.S. infrastructure.
- In March 2005, security consultants within the electrical industry reported that hackers were targeting the U.S. Electric power grid and had gained access to U.S. utilities electronic control systems.
- In April 2009, the Wall Street Journal stated that Chinese and other spies hacked in the U.S. electric grid and left behind computer programs that could allow them to disrupt service.
- Aurora, an experiment to hack control systems and destroy a generator set up the by the Departments of Energy and Homeland Security showed that it was possible (Keogh, 2010).

Patrick Miller, CEO of the National Electric Sector Cybersecurity Organization gives the advantage in a cyber fight to those with malicious intent, saying, “intelligent, adaptive adversaries exist, and they don’t follow the rules or compliance checklists (Miller, 2011).” Companies that have been

successfully attacked recently include Sony, Bank of America, RSA Security, Electronic Arts and Lockheed Martin. Search tools now exist on the internet that allow one to search for internet connected computers at a particular company, making it easier for attackers to find their targets.

Many experts claim the cyber threat is overblown since most SCADA systems are not connected to the internet, i.e., the 'air-gap' theory. The reality is that as hand held devices and internet access become more and more ubiquitous, these systems ***are*** being added to the internet, allowing for more flexible control but increasing the security risk. And, as vulnerabilities are being discovered with these systems, the lack of cyber security within the electrical grid is gaining notoriety. Researchers discovering potential threat vectors have been more than willing to share them openly via the Internet and message boards. Topics at recent hacker conventions have included smart meter hacking and supply chain attacks which has garnered mass media attention and even been the subject of Hollywood movies and TV shows (Miller, 2011).

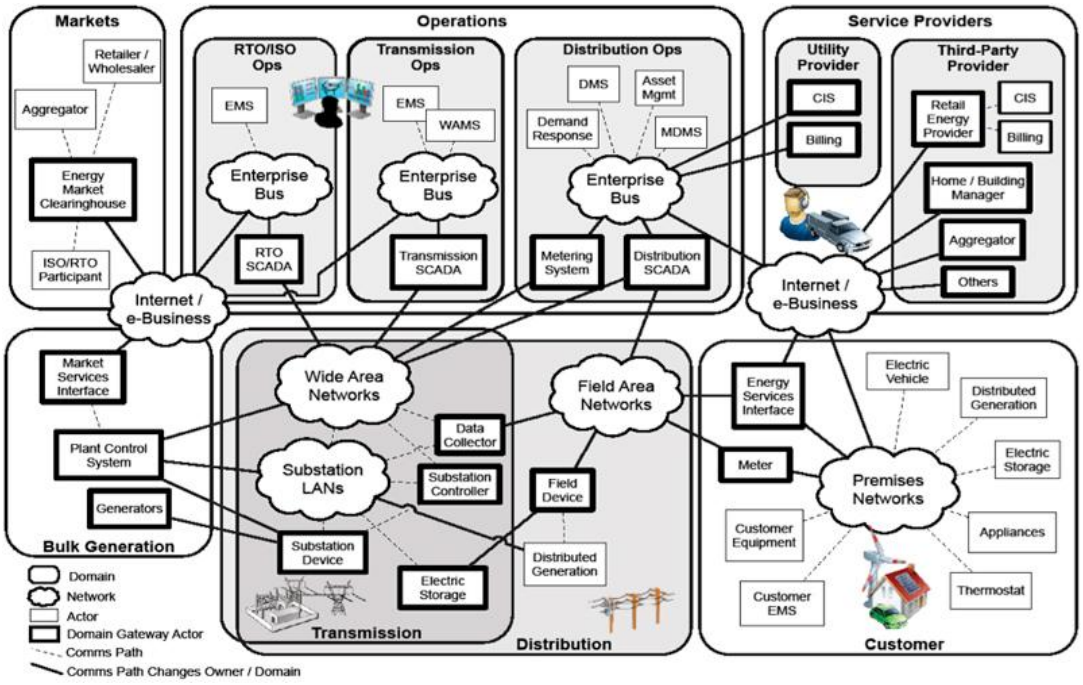
As if these threats were not challenging enough, the electrical industry must also be looking ahead to an even more advanced infrastructure where connectivity is imbedded in almost everything. At the same time they must navigate an ever-changing landscape of regulatory issues: interoperability (how does everything work together?), compliance vs. security issues, data breach disclosure requirements and consumer responsibilities for example. The challenges of cyber security include facing researcher, organized crime and potential nation state attacks while combating the myth of system isolation. Bolting on security to legacy systems is also significantly harder than baking it in.

Information Security

Some of the advantages of smart grid technologies are that it would allow for more resiliency, better efficiency and would detail customer usage down to the appliance level. The trade off for most utilities is that in addition to managing the security of personal payment information they must now be prepared to securely manage the electrical data usage of all of its customers.

As utilities try to reconcile the need to adapt to this new environment, they will be confronted with a whole host of information security issues that will be new. Not only will utilities need to properly manage data security to expected norms, they must also understand the wide range of security threats that could emerge. The following figure shows all the potential ways that electrical data can be transmitted and illustrates the significant problems utilities face in protecting this information from malicious intent.

Figure 9 - Smart Grid Communications



(Lee & Brewer, 2009)

Just some of the areas within information security that utilities need to conscious of include physical security, access controls, communication and transmission security, incident response, disaster recovery and business continuity and network security.

Federal legislation (EISA 2007) includes security in the characteristics of a smart grid:

(1) *Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.*

(2) *Dynamic optimization of grid operations and resources, with full cyber security…* (U.S. Congress, 2007).

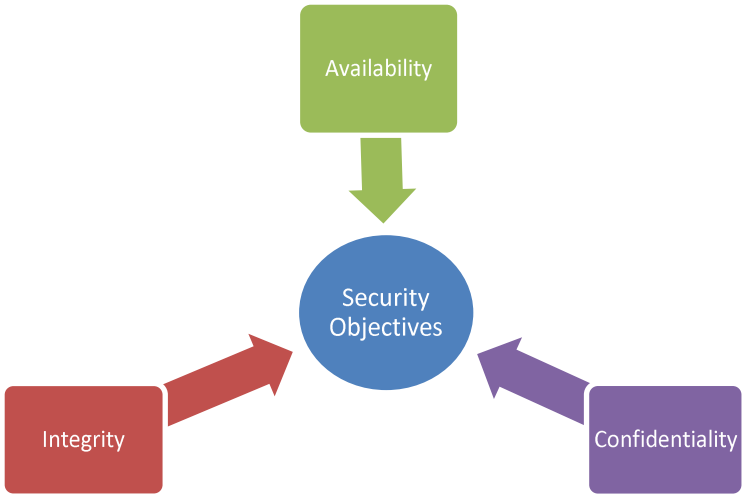
Cyber security involves preventing unauthorized use of, exploitation of, and damage to electronic information and communication systems (National Organization of State Energy Officials, 2011). Restoration of these systems is also a part of cyber security regardless if as part of a deliberate attack or natural event. The overall purpose is to ensure confidentiality, integrity, and availability.

Confidentiality is ensuring that only properly authorized users with a demonstrated need have access to information. This can be implemented in numerous ways, for example: encryption, physical access, classification of information as well as training and education.

Integrity is the assurance that data had not been changed or manipulated without authorization.

Availability means that the information is accessible to authorized users when they need it in the format they need it (Whitman & Mattord, 2009). This 'triangle' of information security can be illustrated in the follow manner:

Figure 10 - The CIA Triangle



(Harris, 2008)

Another area that is sometime added to the 'triangle' is non-repudiation. *Non-Repudiation* is preventing the denial of an action that took place or the claim of an action that did not take place (Keogh, 2010).

Security objectives within an enterprise are ultimately a business decision that is often influenced heavily by legal or regulatory requirements (Stallings & Brown, 2008). Typically a security plan involves four actions: (a) prevention; (b) detection; (c) response; and (d) recovery (Stallings & Brown, 2008). Additionally, the 'users' or customers of an organization's security efforts want a high degree of confidence that those measures are doing what is expected. This, ultimately, is the goal of information assurance: creating and maintaining a high confidence that security measures are providing the protection expected. The CIA triad as framework for an organization's information assurance objectives helps to ensure that that confidence is not misplaced and that those measures meet the business needs of the organization.

There are a number of standards that can be used for developing a smart grid security plan. The following provide guidance in this area:

- NERC CIP Standards 002-009: NERC critical infrastructure protection (CIP) standards for entities responsible for the availability and reliability of the bulk electric system.
- NIST IR 7628: Smart grid cyber security strategy and requirements.
- NIST SP800-53: Recommended Security Controls for Federal Information Systems and Organizations.
- ISO (International Organization for Standardization) 27001, Information Security Management Systems (Lebanidze, 2011).

In order to start developing a security plan, electrical utilities need to identify critical cyber assets. The North American Electric Reliability Corporation defines those as:

- Critical assets: Facilities, systems, and equipment that if destroyed, degraded, or otherwise rendered unavailable would affect the reliability or operability of the bulk electric system.
- Cyber assets: Programmable electronic devices and communications networks including hardware, software, and data.

- Critical cyber assets: Cyber assets essential to the reliable operations of critical assets (NERC, 2008).

Examples of such assets might include generation facilities, transmission substations, control centers, SCADA (Supervisory Control and Data Acquisition) systems, usage data as well as any assets that use a routable protocol (Lebanidze, 2011).

These assets should then be classified in some manner to determine to what level they need to be protected by security controls. An example might be public, restricted, and confidential. Public assets if disclosed would not cause any adverse impact to a company or people. Restricted information is typically reserved for company employees and its release could negatively impact the company's operation and/or security. Confidential information disclosure could seriously affect a company, its mission and security (Harris, 2008).

Personally Identifying Information (PII) is information that could identify the private information of a person. Examples might be their name and social security number, or address; information that when combined could be used to infer who that person is and where they live. Because most utilities use credit card information for billing, they adhere to the PCI Data Standards (Appendix B). While this standard is a private industry initiative, it is expected that in the next legislative session the requirement for compliance will be added to the North Dakota Century Code. Another standard that can be used as guidance for identifying and protecting private information is NIST SP800-12, *Guide to Protecting the Confidentiality of Personally Identifiable Information.*

Table 4 - Data Classification Definitions and Examples

Classification	Definition	Examples
Public	• Disclosure is not desired but would not be adverse to the organization or its personnel	• Current or upcoming projects. • Number of employees.
Restricted	• Has some precautions to ensure integrity and confidentiality of data.	• Financial information • Project details • Earnings and forecast

Confidential	• Company use only • Unauthorized disclosure could seriously affect a company.	• Trade secrets • Competitive information • Health care/Personal information

(Harris, 2008)

Critical cyber assets should all be placed behind an electronic security perimeter (ESP). This 'perimeter' would consist of all of the gateways, routers, firewalls, etc. that impact communications externally. At a minimum, utilities should identify those assets that require an ESP and the access points to each perimeter; for example, firewalls, Virtual Private Network endpoints, web servers, etc. (Lebanidze, 2011).

Once key assets are identified and their boundaries defined, a vulnerability assessment should be done along all of the access points of the ESP. Potential threats, vulnerabilities and risks will be identified that could impact the confidentiality, integrity, or availability of critical cyber assets (Lebanidze, 2011). Most risks fall within one of the following categories: people and policy, process, or technology. Once these risks are identified, the type of impact should be documented. For example, some risks will affect safety; others might cause an outage or monetary damages. Next risks should be ranked by its likelihood. A classification method is shown in table 5.

Table 5 - Risk Level Definitions

Risk Level	Risk Description
Low	The impact to confidentiality, integrity, or availability of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
Moderate	The impact to confidentiality, integrity, or availability of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
High	The impact to confidentiality, integrity, or availability of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

(National Institute of Standards and Technology, 2004)

Next a prioritization strategy to mitigate these risks should be developed based on the potential impact and likelihood. And finally, controls to mitigate these risks should be implemented. Once

controls have been put in place, testing should occur regularly to assess the efficacy of the controls in mitigating the risk.

The controls to manage the indentified risks can run the gamut from the very technical to those much more administrative in nature. Some areas that may not be obvious but can have significant security implications include; hiring and termination practices, change management, password policy, and application controls. Some of the more extensive and technical areas are covered in the following sections.

Physical Security

Hacking systems is not the only way information and assets can be attacked. Physical security is also important, however, this is one area where utilities typically do quite well. Some issues that physical security should address include "site design and layout, environmental components, emergency response readiness, training, access control, intrusion detection, and power and fire protection (Harris, 2008)." Ultimately, physical security is needed to protect **all** of a company's assets from information to people to the actual buildings. Physical security threats include:

1. **Natural environmental threats** Severe weather, flooding, fires, etc.
2. **Supply system threats** Power outages, energy disruptions, etc.
3. **Manmade threats** These can be internal or external – accidents, errors, vandalism, theft, fraud, etc.
4. **Politically motivated threats** Strikes, riots, terrorist attacks, etc. (Harris, 2008)

Good security planning should balance life safety concerns and other security issues. In other words, protecting human life is always the primary concern. It should also be modeled around a defense in depth; if one layer fails, there are others to deter an intruder. At the same time, the CIA (confidentiality, integrity, availability) triangle should drive the development.

A good security plan should also focus on the following goals:

- **Crime and disruption prevention through deterrence** – warning signs, fences, security guards, etc.
- **Reducing damage through the use of delaying mechanisms** – locks, security barriers, guards, etc.
- **Crime or disruption detection** – CCTVs, smoke detectors, heat sensors, etc.
- **Incident assessment** – response of security personnel to incidents or damage
- **Response procedures** – incident response, law enforcement notification plan, etc. (Harris, 2008)

When assessing the physical security of a building, some of the things that should be investigated include:

- HVAC security
- Construction materials
- Power distribution systems
- Communication paths and types (copper, telephone, fiber)
- Surrounding hazardous materials
- Exteriors components:
    - Topography
    - Proximity to airports, highways, railroads
    - Climate
    - Existing fences, cameras, barriers
    - Neighbors
    - Vehicle activity

Each of these areas will need to be assessed in detail. For example, when assessing the construction materials of a building, things like the fire rating, combustibility of material, weight bearing rating, etc. need to be evaluated. Power systems should be examined for potential electromagnetic or radio frequency interference from lighting, motors, etc.

Security zones should also segregate the interior of key buildings. These zones should have requirements and access control in order to enter. Example sets of requirements are shown below:

Figure 11 - Example Security Zone Requirements

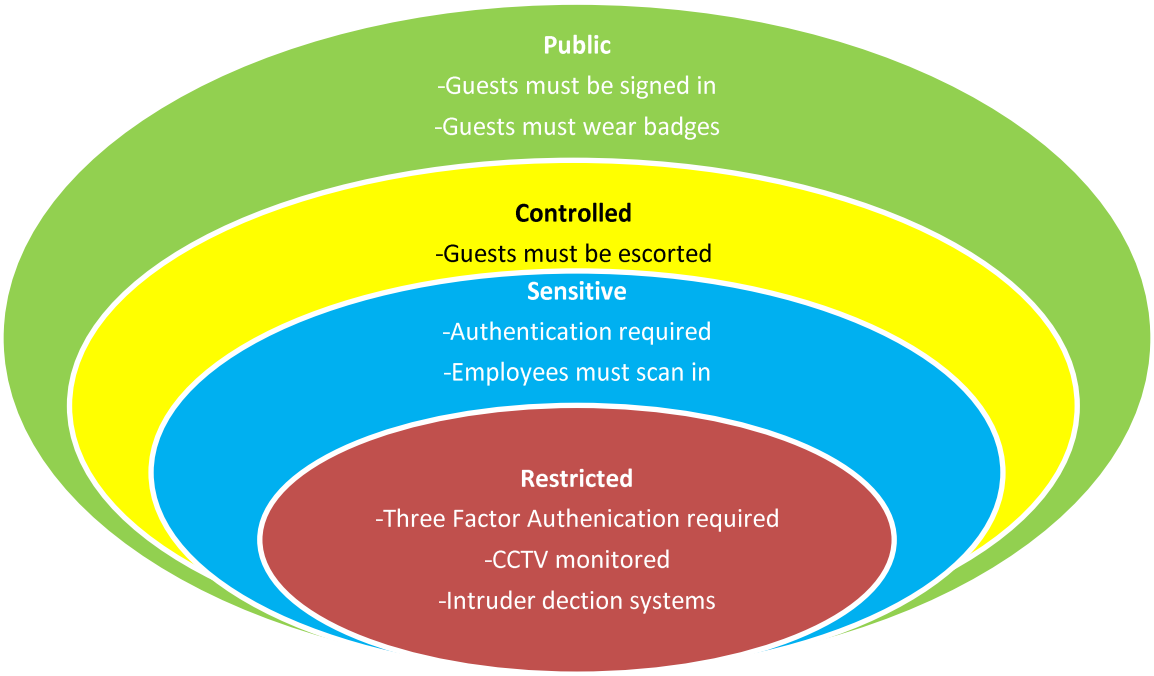


Table 6 - Example Technical Controls

	Technical Controls
Public	ID badges, class 3 locks to rooms
Controlled	Class 2 locks, ID or Employee badges required.
Sensitive	Employee RF Badges Required – Class 1 locks
Restricted	CCTV monitored, mantrap entry, three factor authentication, Class 1 and Intrusion detection.

Once a company has developed and implemented a physical security plan, they should assess that it covers the following areas: deterrence, delay, detection, assessment and response (Harris, 2008). Employees should be trained on the plan and testing should be done to ensure the plan is complete.

Access Controls

Put simply access controls "are security features that control how users and systems communicate and interact with other systems and resources (Harris, 2008)." In order to be allow access to a system or resource a user must go through the following steps; (a) Identification, is the person who they say they

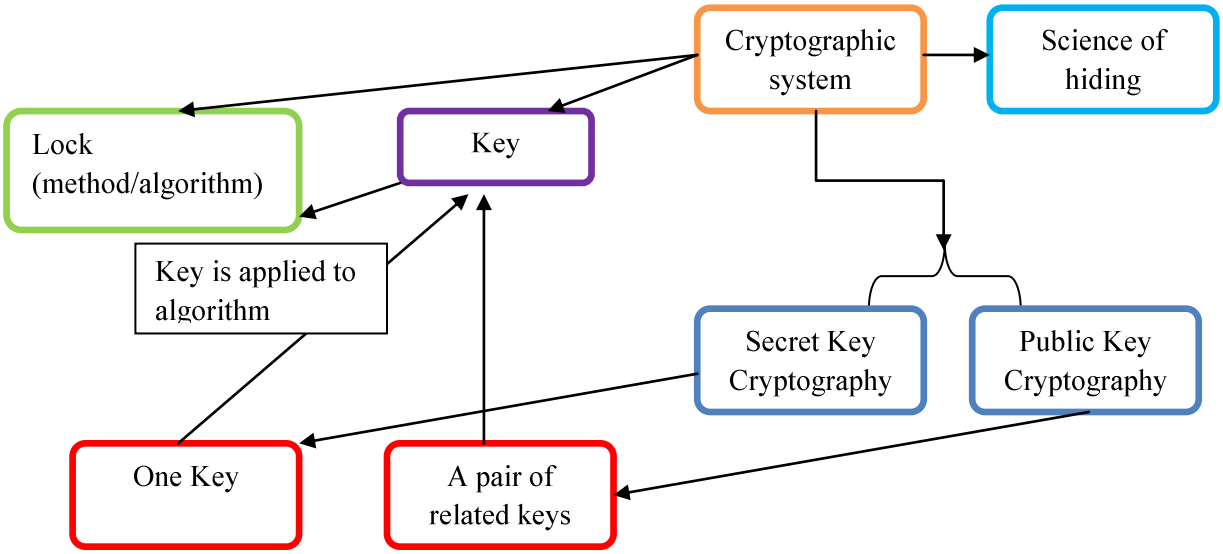
are; (b) Authentication, verification of identification, usually done via a password, token or other piece of identification; (c) Authorization, once properly identified, the system must determine whether the user has the rights and privileges to access the resource; and (d) Accountability, the user is held accountable for any actions taken while access the resource.

The most common form of authentication is a username and password but there are many others that can be used in combination to create a stronger authentication. Typically, authentication requires at least one of three things: something a person knows (a password or PIN), something a person has (a key or swipe card) and something a person is (retina or fingerprint). Strong authentication combines at least two of these methods. Utilities should consider strong authentication for physical as well as application access. Other access controls subjects that the security program should address include password management policy, access control models, administrative controls, and monitoring. Finally, training on what controls are in place and how they should be used should be conducted for all employees.

Communication, Transmission and Network security

Because the communication and transmission of usage data will happen across a wide range of connections (see Figure 9), ensuring the confidentiality and integrity of the data as it travels through these connections is imperative. The most common way is to make sure the data is encrypted during transmission using cryptography. Cryptography, which comes from the Greek work '*kryptos*' (hidden), has an aim "not to hide the existence of a message, but rather to hide its meaning (Singh, 1999)." It is a method of scrambling or *encrypting* a message on one end and then having a way for the recipient to *decrypt* the message upon receipt. The encryption and decryption methods typically involve a mathematical algorithm. A good illustration of the concepts of cryptography is shown below:

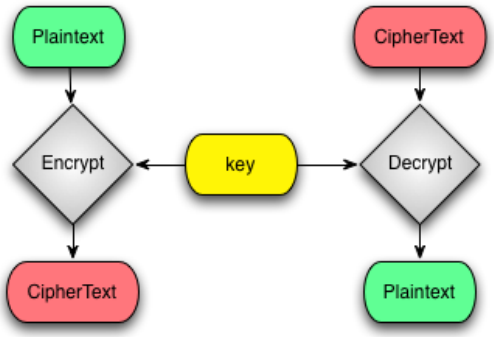
Figure 12 - Cryptography Diagram



(Raval & Fichadia, 2007)

Encryption is taking the plain text message and converting it into ciphertext, a garbled form of the message. This cipher has two components; the algorithm or method used to encrypt the message, and a *key,* which is a variable value that is integral to the encryption method. Decryption is simply a reversal of the encryption method using, in this basic example, the same key. This example describes a secret key or symmetric cryptography method. The important point of this method is that encryption and decryption use the same key which must be agreed upon in advance. While this method of encrypting can be very secure the disadvantage is the distribution of the encryption key. Since the key must be secret for communication to remain private, both parties need the key before being able to establish a secure communication path. A diagram of what this looks like is shown below:

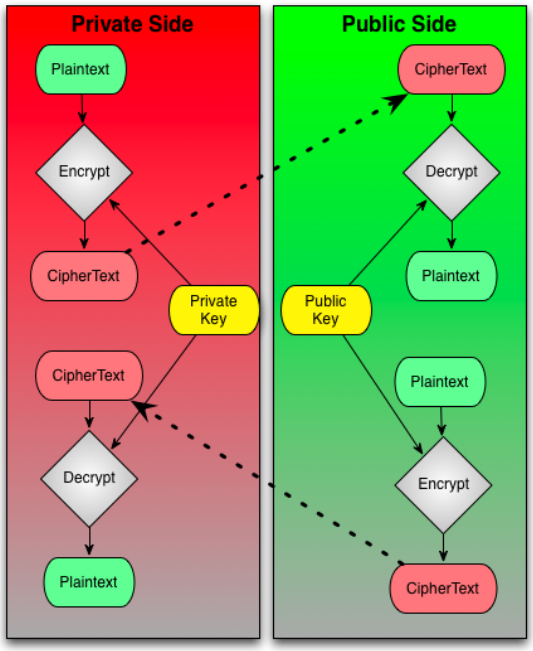
Figure 13 - Symmetric Cryptography



(Chu-Carrol, 2008)

Another method for encrypting is often referred to as public key or asymmetric encryption. This method uses two keys for encryption and decryption of communication. The first is a public key that is shared and is used for encrypting messages. The second is a private key that the receiver keeps decrypting any communication received encrypted with the public key. This is illustrated below:

Figure 14 - Assymetric Cryptography



(Chu-Carrol, 2008)

There are two ways that an algorithm can scramble message content: diffusion and confusion (Raval & Fichadia, 2007). Both make the ciphertext indistinguishable from the plaintext; however, diffusion methods even when complex can often be decrypted using modern day computers. Diffusion typically involves transposition (moving characters backwards or forward) and/or substitution (substituting one of the plaintext characters with another in the alphabet). Confusion is "even more complicated and involves complex transpositions and substitutions" (Raval & Fichadia, 2007).

Cryptography is only one control method for securing communications. Making sure the network over which the data is going to travel is secure is vital. Every part of an information network has an impact to security as they can all introduce potential vulnerabilities. Understanding how network devices, protocols, services, etc. work together will help in identifying the risk (Harris, 2008).

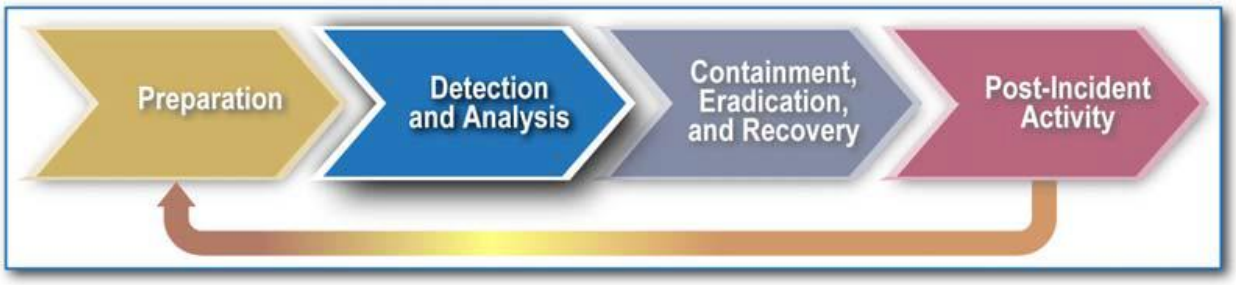
Incident Response

Computer security incidents are an ongoing threat and require due diligence to address accordingly in order to mitigate any potential disruption to state critical infrastructure and retain the confidence of its citizens. In order to ensure a quick and proper response to cyber attacks, utilities should have an incident response plan. A good template for an incident response plan is the National Institute on Standards and Technology (NIST) *Computer Security Incident Handling Guide* (Scarfone, Grance, & Masone, 2008).

The Security Incident Response Team (SIRT) within a utility would handle incident response as well as security advisories, vulnerability assessments, intrusion detection, education and awareness and technology watching.

Incident response should follow the life cycle as shown below:

Figure 15 - Incident Response Lifecycle



(Scarfone, Grance, & Masone, 2008)

Preparation

The incident handling team should ensure that the proper tools and resources are available for handling a security incident. An example list is shown in Appendix C.

Other preparatory activities that can be done to mitigate incidents include:

1. Patch Management. The SIRT should be actively involved in ensuring patches are identified, acquired, tested and deployed.
2. Host Security. Hosts should be given adequate and appropriate hardening.
3. Network Security. The network should only allow necessary activity and all connection points should be secured.
4. User training and awareness. The SIRT should work with IT to help make users aware of procedures and policies as well as appropriate use of the network and applications (Scarfone, Grance, & Masone, 2008).

Detection and Analysis

Because incidents can come in all shapes and sizes, best practice is to prepare to generally handle any type of incident and train to deal specifically with the more common varieties. Some categories that should be planned for include denial of service, malicious code insertion, unauthorized access, inappropriate usage and any combination of these.

The SIRT should be aware of multiple types of incidents and precursors to a possible incident. Examples might include antivirus alerts, buffer overflow attempts, users' complaints of slow network

response, a large volume of bounced emails, or a deviation in network traffic/volume. Understanding what constitutes 'normal' in the daily environment is imperative to identifying when a potential incident might be starting.

Incident Classification

Incidents should be classified and prioritized according to the table below:

Table 7 – Incident Classification

Criticality	Definition	Example
Low	Incidents that *has the potential to have a significant or monumental* impact on the organization's business or service to customers.	Malicious code attacks, including Trojan horse programs and virus infestations
Medium	Incidents that *has a significant* or *has the potential to have a monumental* impact on the organization's business or service to customers.	Password cracking attempts
High	Incidents that *have a monumental* impact on the organization's business or service to customers.	Probes and network mapping

(Osborne, 2001)

Response

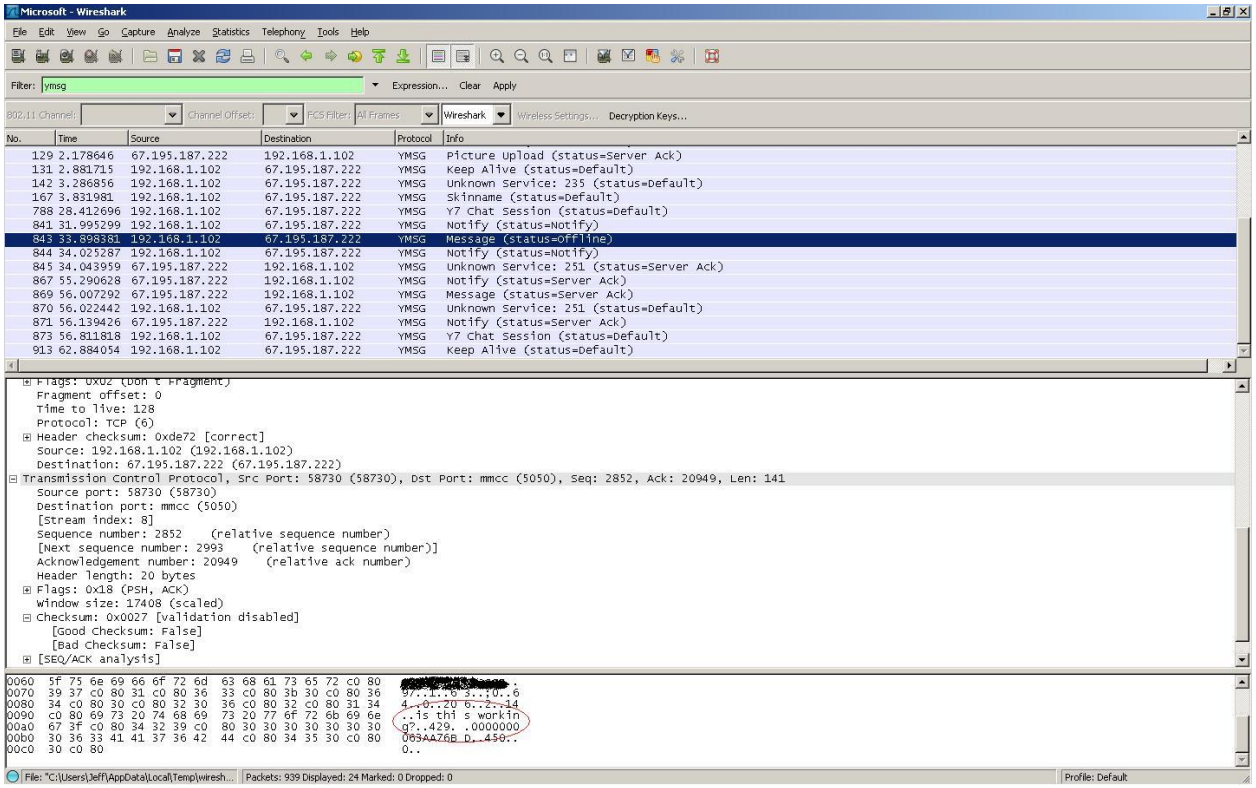
Once an incident has been identified and the appropriate Incident Response Team member notified, the following steps should be taken:

1. Log files.
2. Privileged programs should be verified.
3. Examine for system file tampering.
4. Sniffer Programs started. (see below).
5. Unauthorized services should be identified.
6. Review for password file changes.
7. Check system and network configurations.
8. Look for unusual files.
9. Examine other hosts.

A further incident escalation may be needed. The use of the SANS incident log sheet located on the network drive is preferred to maintain a proper log of the incident (Appendix D).

Once a potential incident has been identified, a sniffer program like Wireshark should be turned on to begin to capture network traffic for analysis. An example screenshot is show in figure 1 below.

Figure 16 - Wireshark Screenshot



(Wireshark)

Follow up

The lead person on the incident response team for each incident is responsible for documenting the incident as well as meeting with the appropriate parties to discuss lessons learned and takeaways from the incident. Questions that should be address include:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?

- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- What corrective actions can prevent similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents? (Scarfone, Grance, & Masone, 2008)

Reporting

All security incidents should be logged and reported. All medium and high criticality incidents should be reported to law enforcement. All high criticality incidents should also be reported to the media through the state Attorney General's office.

Disaster Recovery and Business Continuity

The disaster recovery plan (DRP) is the plan used to recover from a disaster. It is typically focused on information systems but may include areas that are not technology based (Whitman & Mattord, 2009). It is typically one of the main components of the business continuity plan (BCP). The determination of its use vs. that of the incident response plan may be slight but should be defined during contingency planning. This will clearly indicate which plan is activated.

Some of the key considerations or steps to take in creating a DRP are (a) risk analysis, (b), establish the budget, (c) develop the plan, and (d) test (Kunene, 2007).

The National Institute for Standards and Technology (NIST) outlines a seven-step process in SP800-34, Contingency Planning Guide for Information Technology Systems:

1) Develop the DR planning policy statement
2) Conduct the Business Impact Analysis.
3) Identify preventive controls.
4) Develop recovery strategies.
5) Develop the disaster recovery plan document.

6) Plan testing, training, and exercise,

7) Plan maintenance (Swanson, Wohl, Pope, Grance, Hash, & Thomas, 2002).

Business Continuity Plan

A business continuity plan "focuses on sustaining an organization's business functions during and after a disruption" (Swanson, Wohl, Pope, Grance, Hash, & Thomas, 2002). It typically includes the DRP and all business functions. The key point in a BCP is defining "how employees will communicate, where they will go and how they will keep doing their jobs". (Slater, 2009) Derek Slater also lists nine items a BCP should have:

1. Develop and practice a contingency plan that includes a succession plan for your CEO.
2. Train backup employees to perform emergency tasks. The employees you count on to lead in an emergency will not always be available.
3. Determine offsite crisis meeting places and crisis communication plans for top executives. Practice crisis communication with employees, customers and the outside world.
4. Invest in an alternate means of communication in case the phone networks go down.
5. Make sure that all employees-as well as executives-are involved in the exercises so that they get practice in responding to an emergency.
6. Make business continuity exercises realistic enough to tap into employees' emotions so that you can see how they'll react when the situation gets stressful.
7. Form partnerships with local emergency response groups-firefighters, police and EMTs-to establish a good working relationship. Let them become familiar with your company and site.
8. Evaluate your company's performance during each test, and work toward constant improvement. Continuity exercises should reveal weaknesses.
9. Test your continuity plan regularly to reveal and accommodate changes. Technology, personnel and facilities are in a constant state of flux at any company (Slater, 2009, p. 2)

Utilities should evaluate entering into mutual aid agreements that allow for use of nearby facilities if affected by a disaster. A determination would need to be made as to whether the relationship is a timeshare or a straight mutual agreement. A timeshare is "leased in conjunction with a business partner or sister organization. It allows the organization to provide a disaster recovery/business continuity option, while reducing its overall costs (Whitman & Mattord, 2009)." If a mutual agreement is determined to be the best option, some issues should be addressed:

- How long with the facility be available?
- How quickly can the company move in?
- What (if any) are the interoperability issues?
- What resources are available to the company in need?
- How often can the agreement be tested? (Harris, 2008)

An example mutual aid agreement is shown in Appendix E.

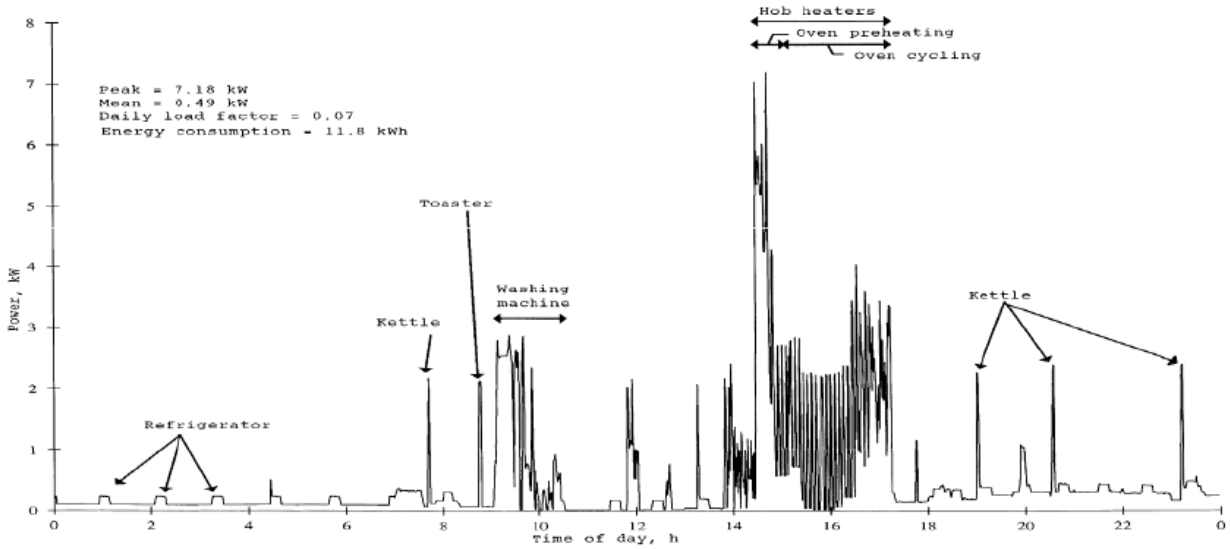
Ethical and Legal Implications

A smarter electrical grid would allow for more resiliency, better efficiency and would detail customer usage down to the appliance level. And therein lies the fear of many privacy advocates; that "information proliferation, lax controls and insufficient oversight of this information could lead to unprecedented invasions of consumer privacy" (Cavoukian, Polonetsky, & Wolf, 2009). Utilities will now have detailed information about when and how your use your electricity. That data, if used incorrectly, could have significant privacy implications for consumers.

What's in the Data?

Tracking consumer electricity usage information is not new. What is new is the level of sampling and detail that can be inferred from the data. An example is shown in Figure 2 below. This chart shows the daily electrical usage for a home in hourly increments. As you can see there is quite a bit that can be determined simply from the usage data. (Bonus points if you can tell the country where this data was taken. Hint: kettle)

Figure 17 - Example Daily Home Electrical Use



Jules Polonetsky, "Privacy and the Smart Grid: New Frontiers, New Challenges" www.futureofprivacy.org, November 2009

Until recently, electrical usage metering relied on the utility reading the meter at the beginning of a billing period and then again at the end. From those numbers, utilities determined the amount used and the peak usage. Any further streamlining of the data required significant guesswork (Quinn, 2009). Because of the current strain on the grid, continued pressure by the Federal government to restrict greenhouse gas emissions, and the need to integrate alternate forms of electricity generation, among other things, utilities are being forced to gather more detailed data to help better utilize power generation and power management. At the same time, consumers want more information in order to more efficiently manage their consumption. All of these needs require a more detailed usage profile. Advanced Metering Infrastructure (AMI) devices, aka smart meters, are the first step toward providing this data.

Now look at the chart in Figure 2 above and think about the following questions:

- When does this person get up?

- When do they come home?
- How do the above times relate to other activities? Example –bar closings, work start time, etc.

A short brainstorming session could probably conjure up several other interesting questions regarding this information, and therein lays the risk.

What are the risks?

Rebecca Harold, one of the leading contributors to the National Institute of Standards and Technology's Smart Grid Interoperability Standards Draft, cited 15 potential privacy concerns related to consumer electrical usage data. They are listed in Table 4.

Table 8 - Privacy Concerns from Smart Grid

Privacy Concern	Discussion
1. Identity Theft	Specific combinations of information may be used to impersonate a utility consumer, resulting in potentially severe impacts, such as negative credit reports, fraudulent utility use and other damaging consumer actions.
2. Determine Behavior Patterns	Access to data use profiles that can reveal specific times and locations of electricity use in specific areas of the home can also indicate the types of activities and/or appliances used. The information revealed is a type of surveillance. The data could be (mis)used by other entities to do target marketing, by governments to try and tax specific activities and uses, and by persons with malicious intent.
3. Determine Specific Appliance Use	Smart meter data will have the ability to track the use of specific smart appliances that are programmed to communicate with the smart meters. Appliance manufacturers may want to get this information to know who, how and why individuals used their products in certain ways. Such information could impact appliance warranties. Insurance companies may want to use this information to approve or decline claims. And there is an unlimited number of other possible uses as yet not imagined that this data could provide.
4. Perform Real-Time Surveillance	Access to live energy use data can reveal if people are in the residence, what they are doing, where they are in the residence, and so on. This not only presents a safety risk, with burglars and vandals using it to their destruction, but it could also be

	used to do target marketing based upon home energy use behaviors.
5. Reveal Activities Through Residual Data	Several articles have been published warning that if the data on the metering devices is not effectively or completely removed, the residual data can reveal to the new meter user, or entity that possess the meter, the activities of the former owner. If true, not only does this present similar concerns to those listed in the first three concern topics, it could also be used by activists or others who have agendas to reveal what they view as a lack of social responsibility. However, to prevent any tampering of historical data and to satisfy the size constraints for the new meters — providing more functionality in the same physical meter box — the data is not likely to be stored within the smart meter itself. But, the possibility of storing data within home meters should be considered in any meter functionality plans so that if it does become possible to store [information] in smart meters the privacy issues will be appropriately addressed.
6. Target Home invasions	Malicious use of meter data for specific consumers could lead to a wide number of problems, such as physical invasions to the home because crooks could tell when residents were away, whether or not they have an alarm system, and so on.
7. Provide Accidental invasions	Combinations of meter data, analyzed for one purpose, could reveal unexpected information about the residents that is then used to the detriment of the residents.
8. Activity Censorship	The meter data could reveal resident activities or uses that utility companies may then subsequently decide are inappropriate or should not be allowed. Without restrictions, if this information could then be shared with local government, law enforcement, or public media outlets the residents could suffer embarrassment, harassment, loss of vital appliances, or any number of other damaging actions.
9. Decisions and Actions Based Upon Inaccurate Data	With meter data being stored in potentially many locations, accessed by so many different individuals and entities, and used for a very wide variety of purposes, it is a significant risk that the data will become inappropriately modified. Automated Smart Grid decisions made for home energy use could not only be detrimental for residents (e.g., restricted power, thermostats turned to dangerous levels, and so on) but decisions about Smart Grid power use and activities could be based upon inaccurate information.

10. Reveal Activities When Used With Data From Other Utilities	Even more personal activities and derived personal information could be revealed if the power meter data was combined with the personal information from other utilities and utility meters, such as those for gas, water, and so on.
11. Profiling	Profiling may be possible in ways that were previously not possible, or not as easily possible. What can you tell about what you can see from energy consumption? For example, if the consumers are straight or gay? Terrorist profiles? Affairs? Illegal activities? Will access to do data mining for investigations put people on terrorist watch lists, etc.? Will politicians want to use for potential activity taxation? Performing a gap analysis could point out scenarios and associated risks.
12. Unwanted Publicity and Embarrassment	Embarrassment and other negative impacts resulting from unauthorized disclosure and/or publication of household or electric vehicle use.
13. Tracking Behaviors of Renters/Leasers	When a different individual owns and pays the utilities other than the resident, such as in the case of a rental unit, room subletting, leasing, and so on, the landlord or property owner could have access to the smart meter data and potentially track the residents' activities. Rent decisions could be made based on past power usage history. Power usage profiling could following individuals and impact a wide range of decisions.
14. Behavior Tracking	Will there be any items within the smart meters that can act in ways similar to browser/document cookies or web bugs? If so, these items could be (mis)used in ways similar to how cookies and web bugs are currently (mis)used. Perhaps RFID tags can be used in some ways? Perhaps GPS types of technologies?
15. Public Aggregated Searches Revealing Individual Behaviors	What kind of smart grid search engines will there be? What discussions or plans have occurred around this possibility? What information would be involved? What control would consumers have to not have their data included in such searches? The privacy issues would be similar to the privacy concerns that currently exist with Internet search engines, only the implications could be more widereaching because the data would be based upon individuals' actual daily living activities, and not upon what they consciously chose to put onto the Internet.

(Herold, 2009)

An overview of Smart Grid data privacy issues shows:

- The privacy implications of the Smart Grid are not yet fully understood.
- There is a lack of formal privacy policies, standards, or procedures by entities that are involved in the Smart Grid and collect information.
- Comprehensive and consistent definitions of personally identifiable information do not generally exist in the utility industry.
- Distributed energy resources and smart meters will reveal information about residential consumers and activities within the house.
- Roaming Smart Grid devices, such as electric vehicles recharging at a friend's house, could create additional personal information.
- Smart meters and the Smart Grid network will be able to use personal information in unlimited numbers of ways.
- Despite the 2000 resolution adopted by the National Association of Regulatory Utility Commissioners urging the adoption of privacy principles, few state level utility commissions have begun to assess privacy and the Smart Grid.
- Future research is necessary and conducting further privacy impact assessments is crucial (Cavoukian, Polonetsky, & Wolf, 2009).

Given these concerns, imagine some of these scenarios:

- Marketing companies targeting ads based on how often you eat in, when you use your computer or watch TV, whether you eat a hot or cold breakfast, and what type of devices you own.
- In court, data is used to determine whether or not you ever leave your kids alone, or how you were able to turn on lights upstairs 1 minute after turning them off downstairs while filing for worker's comp.
- Insurance companies basing your rate on when you get home (near bar close?) or on if you often leave late for work and have to speed to get there on time (Quinn, 2009).

The other risk is simply the danger of unintended consequences that we cannot readily foresee at the present.

Data Protections

According to Elias Quinn, electricity consumption interval data "appears to be in something of a no-man's land under Supreme Court Fourth Amendment jurisprudence (pp 32)". For example, the Court has typically upheld the sanctity of the home when it comes to privacy protection so it could be deduced that electricity usage data should be restricted because in-home activity of consumers could be discovered. However, 'business records collected and kept by third parties enjoy far fewer privacy protections, the underlying theory being that consumers elected to transact with the business, and to engage in activities open to observation by the public. Traditional electricity metering information has generally been treated as business records and so lies unprotected by the Fourth Amendment. (Quinn, 2009)"

What also makes electricity usage information unique is that most of the collection occurs within a regulatory system primarily regulated by state governments and public utility commissions. Unfortunately, these regulations vary wildly from state to state. Colorado, for example, where public utilities such as Xcel Energy are aggressively installing smart meters, does restrict those utilities from disclosing 'personal information'. Disclosure can only come with the consumer's consent. However, the definition of personal information includes "any individually identifiable information obtained by a regulated entity from a customer, from which judgments can be made regarding the customer's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics" as well as "information necessary for the billing and collection of amounts owed to a public utility or to a provider of service using the facilities of a public utility. (Quinn, 2009)" These two definitions would seem to be contradictory when laid against consumer privacy concerns.

There are some federal laws that do influence how utilities should be handling customer information. The Data Protection Rule within the Gramm-Leach-Bliley Act (GLBA) puts requirements on financial institutions' use of customer records and information. The rule is designed to

1. Insure the security and confidentiality of customer data.

2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such data.

3. Protect against unauthorized access to or use of such data that would result in substantial harm or inconvenience to any customer (Reymann & Ashley, 2004).

Additionally, the Sarbanes-Oxley Act of 2002 (SOX) places a significant burden on upper management within publically traded companies to ensure that their financial reporting is accurate. Applicable to this topic, Section 404 of the Act details how companies must monitor and report financial information to include "safeguarding the data and guaranteeing its integrity and authenticity (Harris, 2008)." Compliance failure can result in fines and jail for upper management to include the CEO and CFO.

The National Institute for Standards and Technology noted in their Framework and Roadmap for Smart Grid Standards that there was a "lack of consistent and comprehensive privacy policies, standards and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use creates a very significant risk that must be addressed (Lee & Brewer, 2009)." The National Association of Regulatory Utility Commissioners adopted a resolution in July 2000 aimed at protecting consumer privacy stating that "customers should be permitted to choose the degree of privacy protection" as well as resolving that this data should not be shared with affiliates or third parties. (NARUC, 2000) Unfortunately, few states have even considered the privacy implications of Smart Grid, including North Dakota. This is a huge concern as more and more of these smart meters are put into consumer homes.

Data protections for consumer electricity usage data currently reside in a legal grey area that will need to be clarified as smart grid implementation moves forward. Because this data resides between consumer privacy concerns and the needs of running a business, policy makers will need to consider both sides when developing solutions to the issue. The dilemma is one of concurrently protecting consumer

privacy while ensuring needed technology implementation is not hindered. How the solution is handled will have future implications on technological implementations.

The State's Role

The state plays an important role in ensuring that electrical supply and distribution is assured for its people. Additionally it has a responsibility to ensure an adequate response to cyber security incidents that affect critical infrastructure; working closely with private entities when such incidents occur. Finally through certain state agencies, the state works to advocate for the rights of its citizens.

Emergency Planning and Management

The North Dakota Office of Renewable Energy and Energy Efficiency and the North Dakota Division of Emergency Management are responsible for developing the state's response plan for an energy emergency. The purpose of the plan is to provide timely and coordinated notification to state government, private entities, the media and state residents in the event of an energy emergency. It is also intended to provide appropriate actions to be taken to include, if necessary, enactment of regulations, rules and laws by the state. Principles of the plan focus on addressing the following goals during an energy emergency:

- Ensuring essential services continue to be provided during an energy shortage.
- Responses are prepared/designed to reduce consumption and demand.
- Work with private industry to ensure inequities in distribution of energy is minimized.
- Respond effectively to specific energy disruption conditions.
- Restore a balance of energy products as quickly as possible.
- Assist in mitigating economic hardships caused by an energy disruption.
- Solicit and obtain public support and participation in the plan.
- Deliver timely and accurate information to the public and private industry.
- Create and enact programs, steps, regulation to address the causes of energy emergencies within the state.

The ND Department of Emergency Services along with the Department of Commerce directs all activities in response to an energy emergency, ensuring a coordinated response. The North Dakota Department of Commerce also acts as the maintenance authority for the Energy Assurance Plan and Subject Matter Experts on Energy Assurance issues.

Citizen Advocation

The current North Dakota Century code addresses cyber crime somewhat, but has limited power in regulating business' use of private consumer information. Section 12.1-06.1 of the North Dakota Century Code covers racketeer influenced and corrupt organizations. Within this section definitions are provided for 'access', 'computer', 'computer network', 'computer program', 'computer software' and 'computer system'. The section goes on to detail the state's definition of computer fraud and computer crime and designates such offenses. Computer fraud is a class C felony and computer crime is a class A misdemeanor. It also allows for civil action to be brought for damages, restitution and attorney's fees related to violations of this section (North Dakota Legislature, 2008). Many of the privacy issues that were discussed above will need to be examined by future legislative sessions.

Conclusion

From increased resiliency and reliability to demand management to improved security, smart grid technologies have the capability to transform how we use electricity. It use is not without some potential risks; privacy and security being foremost. However, understanding and educating consumers, public and private entities regarding the benefits and risks of smart grid implementation can only help when it comes to implementation.

GLOSSARY

Term	Definition
Access Control	Security controls that impact how users interact with systems and/or resources.
Advanced Metering Infrastructure	Electrical meters that measure and record usage data at intervals typically less than one hour. Usage data is provided to consumers and utilities at least once per day.
Appliance	An electrical powered piece of equipment used to perform a particular function. Examples include refrigerators, clothes washers/dryers and microwave ovens.
Base Load	The minimum amount of electricity delivered over a period of time.
Business Continuity Plan	The plan for operating business activities in the event of an operations disruption.
CIA triangle	Information Security tenets that include confidentiality, integrity and availability of data.
Critical Cyber Assets	Cyber Assets essential to the operation of critical assets.
Cryptography	A method of hiding the meaning of a message or transmission of data.
Cyber Assets	Programmable electronic devices and networks to include software, hardware and data.
Cyber Security	Information protection from loss, theft or corruption while ensuring availability.
Cyber Security Incident	A malicious act that compromises/disrupts or attempts to compromise/disrupt the electronic security perimeter of a critical cyber asset.
Demand	The rate at which energy is delivered to loads.
Demand Side Management	Activities taken by a utility or customers to influence the amount of electricity they use.

Distribution	The delivery of energy to retail customers.
Disaster Recovery Plan	The plan used to recover from a disaster.
Electric Generator	A facility that produced electricity, measured in kilowatthours (kWh) or megawatthours (MWh).
Electric Power	The rate at which electric energy is transmitted, typically expressed in megawatts (MW)
Electric Power Grid ('Grid')	A system of synchronized power providers and consumers connected by transmission and distribution lines.
Electric Utility	Any entity that generates, transmits, or distributes electricity and recoups its costs through rates set by a regulatory authority.
Electronic Security Perimeter	The border around a network connected to critical cyber assets which also controls access.
Federal Energy Regulatory Commission (FERC)	U.S. Federal agency that has jurisdiction over interstate electrical sales as well as other energy sources.
Generation	The process of producing electrical energy or the amount produced (kWh).
Home Area Network (HAN)	Wireless in-home information network connecting appliances to electronic metering.
Incident Response	Systematic approach to an information security attack.
Interoperability	The ability of diverse electronic systems to work together.
Load	The amount of electric power delivered within a system.
North Dakota Century Code	State law codification.

Off Peak	Time or period of low electrical demand.
On Peak	Time or period of high electrical demand.
Outage	Period of time when generation or transmission is not in service.
PCI Data Standards	Industry accepted standard for properly handling personal credit card information.
Peak Demand (Load)	The highest (max) load during a time period.
Personally Identifying information	Information that can be used to uniquely identify a person.
Phasor Measurement Units	Synchronization device used to measure electricity on a grid.
Physical Security	Measures taken to protect all of a company's assets, not just its data. Examples include building materials, fire response, building design and access control.
Renewable Energy Resources	Energy sources that are naturally replenishing. Examples include hydro, geothermal, solar and wind.
Risk	The likelihood that a vulnerability is exploited with a negative impact to the business.
SCADA	A system of remote control used to monitor and control electrical transmission systems.
SIRT	Security Incident Response Team – responsible for coordinating the approach to a security incident.
Smart Grid	An improved electrical grid that shares information in two directions.
Surge	A temporary variation of voltage, current or flow in an electrical circuit.

Threat	Any potential danger to data or systems.
Transmission	A connected group of lines and equipment used for the movement of electricity between generation and consumption points.
Virtual Private Network	A secure, private connection through a public unsecured network.
Vulnerability	A weakness that an attacker can exploit to gain unauthorized access to a system or resources.

(Harris, 2008) (NERC, 2008) (U.S. Department of Energy, 2008)

References

Amin, M. (2008). Upgrading the Grid. *Nature* , 570-573.

Cavoukian, A., Polonetsky, J., & Wolf, C. (2009, November). *Smart Privacy for the Smart Grid: Embedding Privacy in to the Design of Energy Conservation.* Retrieved November 18, 2010, from http://www.ipc.on.ca: www.ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf

Chandra, V. (2009). *Electrical Generation.* Retrieved February 13, 2012, from http://www.natgas.info: http://www.natgas.info/html/gasusage.html

Chu-Carrol, M. C. (2008, November 20). *http://scienceblogs.com.* Retrieved October 19, 2011, from Assymmetric Cryptography: the Basic Idea of Public Key Cryptosystems:Good Math, Bad Math: http://scienceblogs.com/goodmath/2008/11/asymmetric_cryptography_the_ba.php

Coleman, D. D., Westcott, D. A., Harkins, B. E., & Jackman, S. M. (2010). *CWSP: Certified Wireless Security Professional - Official Study Guide.* Indianapolis, Indiana: Sybex/Wiley Publishing.

Danahy, J. (2009, October). *Smart Grid for the CSO.* Retrieved November 15, 2010, from http://www.smartgridsecurityblog.com: http://smartgridsecurity.blogspot.com/2009/11/smart-grid-intro-for-csos.html

Donovan, L. (2011, May 3). *Getting the power back.* Retrieved February 3, 2012, from http://www.bismarcktribune.com: http://bismarcktribune.com/news/state-and-regional/article_d1887e5a-7548-11e0-9281-001cc4c03286.html

Energy Information Administration. (2012, January 27). *North Dakota Electricity Profile*. Retrieved January 28, 2012, from http://www.eia.doe.gov: http://www.eia.gov/electricity/state/northdakota/

Energy Information Administration. (2009, June 26). *U.S. Primary Energy Consumption by Source and Sector, 2008.* Retrieved November 16, 2009, from http://www.eia.doe.gov: http://www.eia.doe.gov/emeu/aer/pecss_diagram.html

Harris, S. (2008). *CISSP All-in-One Exam Guide, Fourth Edition.* New York: McGraw-Hill.

Herold, R. (2009, October). *Smart Grid Privacy Concerns.* Retrieved November 29, 2009, from http://www.privacyguidance.com: http://www.privacyguidance.com/files/SmartGrid_PrivacyHeroldOct2009.pdf

Kalkunte, V. (2010, September 25). *Role of Wifi/IEEE 802.11n & Related Protocols in Smart Grid.* Retrieved November 19, 2010, from http://ewh.ieee.org: http://ewh.ieee.org/r6/scv/comsoc/Workshop_092510_11nInSG.pdf

Keogh, M. (2010, December 16). *Cyber Security and Energy Assurance.* Retrieved December 15, 2011, from http://www.naseo.org: http://www.naseo.org/energyassurance/webinars/Smart_Grid_Cyber_Security_for_Energy_Assurance_Webinar-2010-12-16.pdf

Kunene, G. (2007). *How to Create a Disaster Recovery Plan.* Retrieved August 16, 2009, from http://www.devx.com: http://www.devx.com/security/Article/16390/1954

Lebanidze, E. (2011). *NRECA Guide to Developing a Cyber Security and Risk Mitigation Plan.* Retrieved January 7, 2012, from http://www.nreca.coop: https://groups.cooperative.com/smartgriddemo/public/CyberSecurity/Pages/default.aspx

Lee, A., & Brewer, T. (2009). Smart Grid Cyber Security Strategy and Requirements - DRAFT. *National Institute for Standards and Technology* , 8-10.

Miller, P. C. (2011, August 31). *Threats, Vulnerabilities and Impacts: Energy Security in the Digital Age.* Retrieved January 15, 2012, from http://doe-oe-regionalexercies2011.govtools.us: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6enr.txt.pdf

NARUC. (2000). *www.naruc.org.* Retrieved December 6, 2009, from Resolution Urging the Adoption of General Privacy Principles For State Commission Use in Considering the Privacy implications of the Use of Utility Customer Information: http://www.naruc.org/Resolutions/privacy_principles.pdf

National Institute of Standards and Technology. (2004, February). *FIPS-199.* Retrieved May 5, 2011, from http://csrc.nist.gov: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

National Organization of State Energy Officials. (2011, November). *Smart Grid and Cyber Security for Energy Assurance.* Retrieved February 15, 2012, from http://www.naseo.org: http://www.naseo.org/energyassurance/NASEO_Smart_Grid_and_Cyber_Security_for_Energy_Assurance_rev_November_2011.pdf

National Organization of State Energy Officials. (2009, December). *State Energy Assurance Guidelines.* Retrieved May 2010, from http://www.naseo.org: http://www.naseo.org/eaguidelines/State_Energy_Assurance_Guidelines_Version_3.1.pdf

NERC. (2008, February 12). *Glossary of Terms Used in Reliability Standards.* Retrieved February 19, 2012, from http://www.nerc.com: http://www.nerc.com/files/Glossary_12Feb08.pdf

North Dakota Legislature. (2008). *North Dakota Century Code.* Retrieved January 11, 2011, from Title 12.1 Criminal Code: http://www.legis.nd.gov/cencode/t121c061.pdf

Osborne, T. R. (2001). *www.sans.org.* Retrieved September 8, 2009, from Building an Incident Response Program To Suit Your Business:

http://www.sans.org/reading_room/whitepapers/incident/building_an_incident_response_program_to_suit_your_business_627?show=627.php&cat=incident

Quinn, E. L. (2009, February). *PRIVACY AND THE NEW ENERGY INFRASTRUCTURE.* Retrieved November 23, 2009, from http://ssrn.com: http://ssrn.com/abstract=1370731

Raval, V., & Fichadia, A. (2007). *Risks, Controls, and Security: Concepts and Applications.* Hoboken, NJ: John Wiley and Sons.

Reymann, P., & Ashley, M. (2004, July). *The Data Protection Rule of the Gramm-Leach-Bliley Act: A strategy for compliance.* Retrieved June 3, 2011, from http://www.stillsecure.com.

SANS. (2003). *Computer Security Incident Handling Form.* Retrieved May 16, 2011, from http://www.sans.org: http://www.sans.org/score/incidentforms/IH_Identification.pdf

Scarfone, K., Grance, T., & Masone, K. (2008, March). *Computer Security Incident Handling Guide.* Retrieved May 13, 2011, from http://csrc.nist.gov/: http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

Security Manager Plus. (2011). *PCI DSS Compliance Checklist.* Retrieved June 3, 2011, from http://www.manageengine.com: http://www.manageengine.com/products/security-manager/pci-dss-compliance-checklist.html

Siddiqui, O. (2008, June). *The Green Grid: Energy Savings and Carbon Emissions Reductions Enabled by a Smart Grid.* Retrieved January 30, 2011, from http://www.epri.com: http://my.epri.com/portal/server.pt?space=CommunityPage&cached=true&parentname=ObjMgr&parentid=2&control=SetCommunity&CommunityID=404&RaiseDocID=000000000001016905&RaiseDocType=Abstract_id

Singh, S. (1999). *The Code Book.* New York, New York: Anchor Books.

Slater, D. (2009, May 7). *Business Continuity and Disaster Recovery Planning: The Basics.* Retrieved August 16, 2009, from www.csoonline.com: http://www.csoonline.com/article/print/204450

Stallings, W., & Brown, L. (2008). *Computer Security: Principles and Practice.* Upper Saddle River, NJ: Prentice Hall.

Sullivan, B. (2009). *http://www.msnbc.com.* Retrieved October 25, 2009, from What will talking power meters say about you?: http://redtape.msnbc.com/2009/10/would-you-sign-up-for-a-discount-with-your-power-company-in-exchange-for-surrendering-control-of-your-thermostat-what-if-it.html

Swanson, M., Wohl, A., Pope, L., Grance, T., Hash, J., & Thomas, R. (2002, June). Contingency Planning Guide for Information Technology Systems. *NIST sp800-34* . Gaithersburg, Maryland: National Institute of Standards and Technology.

U.S. Congress. (2007, January 4). *Energy Independence and Security Act of 2007.* Retrieved February 19, 2012, from http://frwebgate.access.gpo.gov: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6enr.txt.pdf

U.S. Department of Energy. (2011, August 2011). *Demand Dispatch - Intelligent Demand for a More Efficient Grid.* Retrieved February 16, 2012, from http://www.netl.doe.gov: http://www.netl.doe.gov/smartgrid/docs/DemandDispatch_08112011.pdf

U.S. Department of Energy. (2008). *The Smart Grid: An Introduction.* Litos Strategic Communications.

Whitman, M. E., & Mattord, H. J. (2009). *Management of Information Security.* Boston, MA: Thomson Course Technology.

Wireshark. (n.d.). *About Wireshark.* Retrieved October 11 2010, from http://www.wireshark.org: http://www.wireshark.org/about.html

APPENDIX A HOME ENERGY CONTROLLER EXAMPLE

Cisco Home Energy Controller (HEC)

Feature	Specification
Display	7 inch wide screen 24 bit color TFT LCD 800 x 480 Capacitive-touch, Active matrix LCD panel with LED backlighting Viewing Angles: 130 deg horizontal, 110 deg vertical Aspect Ratio: 15:9
Processor	1.1 GHz Intel Atom-includes hyper-threading and integrated GPU
Memory DDR2 ECC DRAM	512 MB running at 533 MHz
Storage (Flash): mNAND	1-2 GB (factory expandable to 64 GB)
Ethernet	10/100/1000 base-TX with RJ45 connector on rear of unit
Cryptography	SSL Implemented in software hardware used on some Intel chips
WiFi 802.11 b/g/n	Integrated via PCIe WMM QoS WEP, WPA, WPA2 encryption

APPENDIX B PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS)

The Standard requires that companies meet the following requirements:

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security (Security Manager Plus, 2011)

APPENDIX C INCIDENT HANDLING RESOURCE LIST

Acquired	Tool/Resource
	Incident Handler Communications and Facilities
	Contact information for team members and others within and outside the organization (primary and backup contacts), such as law enforcement and other incident response teams; information may include phone numbers, email addresses, public encryption keys (in accordance with the encryption software described below), and instructions for verifying the contact's identity
	On-call information for other teams within the organization, including escalation information (see Section 3.2.6 for more information about escalation)
	Incident reporting mechanisms, such as phone numbers, email addresses, and online forms that users can use to report suspected incidents; at least one mechanism should permit people to report incidents anonymously
	Pagers or cell phones to be carried by team members for off-hour support, onsite communications
	Encryption software to be used for communications among team members, within the organization and with external parties; software must use a Federal Information Processing Standards (FIPS) 140 validated encryption algorithm
	War room for central communication and coordination; if a permanent war room is not necessary, the team should create a procedure for procuring a temporary war room when needed
	Secure storage facility for securing evidence and other sensitive materials
	Incident Analysis Hardware and Software
	Computer forensic workstations[33] **and/or backup devices** to create disk images, preserve log files, and save other relevant incident data
	Laptops, which provide easily portable workstations for activities such as analyzing data, sniffing packets, and writing reports
	Spare workstations, servers, and networking equipment, which may be used for many purposes, such as restoring backups and trying out malicious code; if the team cannot justify the expense of additional equipment, perhaps equipment in an existing test lab could be used, or a virtual lab could be established using operating system (OS) emulation software
	Blank media, such as floppy disks, CD-Rs, and DVD-Rs
	Easily portable printer to print copies of log files and other evidence from non-networked systems
	Packet sniffers and protocol analyzers to capture and analyze network traffic that may contain evidence of an incident
	Computer forensic software to analyze disk images for evidence of an incident
	Removable media with trusted versions of programs to be used to gather evidence from systems
	Evidence gathering accessories, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions
	Incident Analysis Resources
	Port lists, including commonly used ports and Trojan horse ports
	Documentation for OSs, applications, protocols, and intrusion detection and antivirus signatures
	Network diagrams and lists of critical assets, such as Web, email, and database servers
	Baselines of expected network, system and application activity
	Cryptographic hashes of critical files[34] to speed the analysis, verification, and eradication of incidents

(Scarfone, Grance, & Masone, 2008)

APPENDIX D SANS INCIDENT LOG SHEET

General Information

Incident Detector's Information:

Name:_____ Date and Time Detected: _____
Title: _____

Phone:_____ Alt. Phone: _____ Location Incident Detected From: _____
Mobile: _____ Pager:_____ _____
Fax:_____ Alt. Fax:_____ Additional Information:_____

E-mail: _____ _____
Address: _____ _____
_____ _____

Detector's Signature:_____ Date Signed: _____

Incident Summary

Type of Incident Detected:

- Denial of Service
- Unauthorized Use
- Espionage
- Probe
- Hoax
- Malicious Code
- Unauthorized Access
- Other:_____

Incident Location:

Site:_____ How was the Incident Detected:_____

Site Point of Contact:_____ _____

Phone:_____ Alt. Phone: _____ _____
Mobile: _____ Pager:_____ _____
Fax:_____ Alt. Fax:_____ _____
E-mail: _____ _____

Address: _____ _____
_____ _____

Additional Information: _____
_____
_____

(SANS, 2003)

APPENDIX E EXAMPLE MEMORANDUM OF AGREEMENT

MEMORANDUM OF AGREEMENT BETWEEN
COMPANY X
AND
GREAT RIVER CORPORATION

1. Purpose

The purpose of this agreement is to enter into a cooperative relationship with Great River Corporation which would allow Company X temporary access to available office space in the Great River building located at 1554 State Street for the purpose of temporarily relocating essential office functions and recovery management following a disaster which renders the existing Company X facility unusable.

This agreement sets for the intent and basic relationship for both parties, it does not, however, represent a legal obligation binding the parties to any fiscal or performance related commitments. It is expected that a lease would be executed at the time of activation of this contingency agreement.

2. Governing Principals

- The occupancy of Great River facilities by Company X will be for a temporary basis and subject to the mutual agreement of Great River and Company X.
- The Great River facilities will include the 4 large conference rooms on the second floor and any space Great River could make available to Company X.
- The occupancy of Great River facilities will be for essential office functions as defined by the Company X COOP plan and for essential recovery management staff.
- Compensation to Great River for the use of their space will be determined by mutual agreement at the time activation occurs. This would require a typical rental/lease and reflect current costs.
- Once activation becomes necessary, Company X will provide notification to Great River through specified contacts or their representatives.
- It is expected that it may take some time for Company X to prepare to move and for Great River to be ready to receive Company X personnel.
- Company X will be responsible for all charges related to the relocation and any IT/communication connections and associated costs.
- It may be necessary in the short term to use existing furniture within the Great River conference rooms until Company X can acquire the proper furnishings/equipment.
- If Company X equipment such as a copier or fax machine is not yet available at time of occupancy, Company X will reimburse Great River for the use of any equipment allowed by Great River.

3. Notification Procedures

Upon the activation of the Company X COOP plan, Great River will be contacted by Company X through the contacts listed below:

Great River (Primary):	**Company X (Primary):**
Peg Boyd, Executive Director	Steve Anderson, President
Great River Corporation	Company X
1554 State Street	1 Capitol Way
Bismarck, ND 58501	Bismarck, ND 58501
Phone number	Phone number
Email	Email
Secondary Contact	Secondary Contact

4. Effective date/Review/Termination

This agreement becomes effect when signed by both parties. It shall be reviewed biennially and may be amended with mutual agreement. Either party may terminate the agreement with written advance notice to the other party.

5. Signatures

_____ Date_____

_____ Date_____